ABSTRACT OF THE DISCLOSURE

A digital data file encryption apparatus and method, where a digital data server identifies the user and supplies an encrypted digital data file to the user in accordance with the identified result. A personal computer decrypts the encrypted digital data file supplied from the digital data server and reproduces the decrypted digital data file or re-encrypts it using an encryption key. The encryption key is generated on the basis of an identification number of a data storage medium or digital data playing device. A digital data playing device stores the re-encrypted digital data file downloaded from the personal computer in the data storage medium and decrypts the stored digital data file using the encryption key to reproduce it. A first internal key is added to the identification number to convert the identification number into the encryption key, which is then encrypted according to an encryption algorithm based on a second internal key. The digital data file is the encrypted using the encrypted encryption key.